IN THE CLAIMS:

Claims 1 to 51 have been cancelled in prior amendments.

52. (currently amended) A payment card for conducting a payment transaction between a customer and a merchant that protects the customer identity data by not having customer identity data on the card itself and not transferring such data to a merchant during a payment transaction, the payment card comprising:

a. a substrate without a computer processing ability as in a microprocessor;

b. an alias name printed on the substrate, the alias name being selected by the customer;

c. a customer-identifier, permanently identifies the customer to a payment system that is without customer identity of name and bankcard number, encoded on an encoding medium on the substrate, whereby the payment card does not have customer identity data and thus does not transfer such data to a merchant during a payment transaction.

53. (previously presented) The claim as in 52, comprising:
the encoding medium is a magnetic strip.

54. (previously presented) The claim as in 52, comprising:
the customer-identifier is self-created by the customer.

55. (previously presented) The claim as in 52, comprising:
the customer-identifier identifies the customer to a payment system, wherein the customer has an account and has pre-stored his/her bankcard data identifying each bankcard with a card specific personal identification number (CPIN).

56. (previously presented) The claim as in 52 [[55]], comprising:

[~~the payment system assigns~~] an algorithm[~~, the algorithm being~~] used to encrypt the customer-identifier, the encrypted customer-identifier appended with a reference to the algorithm is encoded on the payment card as an encrypted customer-identifier, and the card is physically delivered to the customer.

57. (previously presented) The claim as in 55, comprising:

the customer swipes the card at a merchant Point-Of-Sale (POS) terminal, enters the CPIN, to effect a payment to the merchant from a bankcard identified by the CPIN.

58. (previously presented) The claim as in 57, comprising:

the POS terminal transfers the customer-identifier, the CPIN, a merchant identifier, and a payment amount to a gateway to a bankcard authorization network (bankcard processor), wherein the bankcard processor interfaces with the payment system using the customer-identifier and the CPIN

59. (previously presented) The claim as in 58, comprising:

the payment system uses the customer-identifier to identify customer in the payment system and with the CPIN retrieves specific bankcard data selected by the customer and sends it to the bankcard processor.

60. (previously presented) The claim as in 59, comprising:

the bankcard processor processes the payment transaction between the customer and the merchant, and sends payment approval data to the merchant POS terminal.

61 to 66 have been cancelled in this amendment .

67. (currently amended) A payment system that protects customer identity data from theft in merchant systems, comprising:

a. a server capable of high volume storage and database searches;

b. the server maintains a database having a permanent customer-identifier for a customer and tied to this customer identifier, at least two bankcard accounts data of the customer and for each bankcard account, a customer selected [[~~plurality of accounts each identified with a customer-identifier and stores at least one bankcard data of the customer and a customer assigned~~]] card specific personal identification number (CPIN);

c. the system receives [~~the customer-identifier and the CPIN from a merchant point of sale (POS) for a payment transaction ,verifies the customer, retrieves the specific bankcard data identified by the CPIN, and submits a payment transaction record to a prior art card processor network~~] an encrypted data record from a merchant point of sale (POS) for a payment transaction, where a payment card is swiped and a specific CPIN entered by the customer in the point of sale, the record having the customer-identifier from the card and the entered CPIN, the payment system decrypts the record and identifies and verifies the customer in the database and retrieves the specific bankcard data of the customer that is identified by the CPIN, and submits a payment transaction record to a prior art card processor network, thereby the payment system enables a customer to carry this one payment card only and use it in lieu of his one or the other bankcard in the payment system, and protect customer identity data from potential theft in merchant systems.

68 to 70 are cancelled in this amendment.

71. (currently amended) A payment transaction method between a customer and a merchant equipped with a point of sale (POS) terminal for accepting payments comprising the step of:

swiping a payment card at the POS terminal by a customer with the payment card encoded with a customer-identifier, without customer identity of name and bankcard number;

[[and]] entering a card specific PIN for selecting a specific bankcard for this payment transaction from [~~a plurality of~~] at least two bankcards of the customer that are pre-stored in a payment system; [~~, for this payment transaction~~.]

receiving payment transaction data from the POS terminal by a bankcard processor, interfacing with a payment system with the customer-identifier and the CPIN and retrieving the bankcard data intended for the payment transaction;

processing payment transaction by the bankcard processor and sending payment approval data to the merchant POS terminal, thereby the method enabling the customer to use one private payment card in lieu of other bankcards.

72 to 73 cancelled in this amendment.

74 to 76 cancelled in prior amendments

77. (currently amended) A method of selecting any one of at least two [~~a plurality~~] of bankcards of a customer at a merchant point of sale for a payment to a merchant comprising the steps of:

a. entering of a customer identifier , without customer identity of name and bankcard number, and a bankcard specific personal identification number (CPIN) in the point of sale interface;

b. sending the identifier and the CPIN to a card processor;

c. interfacing by the card processor with a payment system, wherein the customer having at least two [~~a plurality of~~] pre-stored customer bankcard data, each bankcard identified with the CPIN;

d. returning to the card processor the bankcard data corresponding to the customer identifier and the CPIN from the payment system.

78. (previously presented) The Claim as in 77, having further step of:

identifying a particular bankcard of the customer and verifying the customer by the CPIN.

79. (previously presented) The claim as in 77, having further step of:

processing the payment transaction with the bankcard data by the card processor.

80. (previously presented) The claim as in 78, having further steps of:

a. having access to the payment system by the customer;

b. entering the bankcard data and self-selecting a CPIN for each bankcard of the customer.

Claims 81 to 83 have been cancelled in prior amendment.
Claims 84 and 85 are cancelled in this amendment

86. (newly added) A system of identity security in use of bankcards, comprising:

a. an identity security system having a customer identifier that is without customer name and bankcard data;

b. the customer identifier anchoring at least two bankcard data of the customer each identified with a CPIN;

c. encrypting the customer identifier with an aliasing algorithm from a list of such algorithms in a database maintained by the security system;

d. encoding the encrypted identifier and the algorithm reference number on a payment card encoding mechanism.

87. (newly added) The system of identity security in use of bankcards as in claim 86, further comprising:

the system, on receiving from a merchant POS, the encrypted customer identifier by swiping of the card and entry of a CPIN, selecting the CPIN specific bankcard data for processing a payment transaction with a prior art payment network, thereby the identity security system does not identity the customer and customer bankcard data to the merchant system.

88. (new) A merchant point-of-sale terminal that protects customer identity data from potential theft, comprising:

a. a wireless point-of-sale (WPOS) terminal that protects customer identity data from potential theft, by providing a secure wireless connection for the transfer of a payment authorization transaction record directly to a payment system that is not a merchant system and receive payment approval data, the payment system having received it from a prior card authorization network;

b. the WPOS has a wire line merchant interface for receiving merchant id data and a payment amount for a specific transaction and for transfer of the payment approval data to the merchant system.

89. (new) The merchant point-of-sale terminal as in claim 88, further comprising:

the WPOS receives customer identifier data, that is without a name and bankcard data, from a payment card and a card specific PIN from the card owner at the time of payment transaction, combines that with merchant id data, dollar amount and a transaction identifier and encrypts the record before wirelessly transmitting to a payment system.

90. (new) The merchant point-of-sale terminal as in claim 88, further comprising:

a. the WPOS has card reader mechanism, a keypad, a display screen, and foldable privacy shields around the keypad and the display screen for receiving customer payment card data;

b. the WPOS has memory for temporarily holding payment authorization data record and payment approval data record.

91. (newly added) A method of secure data storage of a bankcard number comprising the steps of:

a. transforming the original bankcard number data string into a transformed data string, the transformed data string having format attributes making it indistinguishable from the original data string, wherein the transforming means include (i) parsing the bankcard number into its parts of bank identification number, card number and expiration date, (ii) having a table A of bank identification numbers and a table B of expiration dates, (iii) looking up the bank identification number location in the table A, applying a random number (RN1) to the location, using the new location looking up a transformed bank identification number, (iv) applying a random number (RN3) to the card number to get transformed card number, (v) looking up the expire date location in the table B, applying a random number (RN2) to the location, using new location looking up a transformed date, (vi) composing a transformed bankcard number made from transformed bank identification number, transformed card number and transformed expiration date;

b. saving the transformed bankcard number and the transform sequence of RN1, RN2, and RN3 in data storage by a reference number.

92. (newly added) The claim as in 91, comprising the step of: storing the transform sequence in separate data storage means than the transformed bankcard number.

93. (newly added) The claim as in 92, comprising the step of: supplying the reference number, reading the transformed bankcard number and transform sequence, and performing reverse steps to assemble the original bankcard number.